Lecture 1
Course Overview and Introduction

CS3690 Network Security
Summer Quarter, 2000
C. Irvine

Objectives

- Introductions
- Course Plan
- Expectations
- Questions

Introduction - Course and Instructor

- Course
  - ★ CS 3690 - Network Security
  - ★ Prerequisites
    - CS3600
    - Introduction to computers
    - Introduction to networking
  - ★ homepage:
    - http://www. cs .nps.navy.mil/people/ ffaculty/irvine/classes/CS3690
- Instructor
  - ★ Cynthia Irvine
    - Office: Sp 528a
    - e-mail: irvine@cs .nps .navy.mil
    - Office Hours

Weekly Schedule and Special Dates

- July 18 Bill Murray Visit
- July 27 Brett Chappell Visit
- August 3 and 4
- August 11

Course Sketch

- Objective: examine network security from the perspective of tools and their usage. Understanding of threats and how they can be addressed.
- Components and Tools include:
  - ★ hardware/software
  - ★ engineering and scientific analysis
  - ★ operating systems
  - ★ cryptography
  - ★ communication protcols
  - ★ network and resource management
- Discussion Strongly Encouraged

Lecture Plan I

- Introduction
- Network Threats and Vulnerabilities
- Trust and Ntworks
- Why Modern Cryptography Works
- Cryptography Basics
- Block Ciphers Modes and Uses
- Cryptanalysis and Cipher Strength
- Hashing, Digital Signatures I
- Steganography
- Random Numbers and Number Theory
- Exam

Lecture Plan II

- Public Key Cryptography
- Public Key Variations and ECC
- Key Management
- PKI
- Network Security Placement
- IPSec and VPNs
- SSL/TSL
- Cookies, Data Aggregation and Privacy
- Privacy Technologies
- Network Authentication
- Exam

Lecture Plan III

- Kerberos and Similar Systems
- Tokens and Smartcards
- Coherent Network Security
- Mobile Code and Mobile Devices
- Guards, Filtering Guards, and Firewalls
- Security for Dynamic Coalitions
- Application-level Security
- Intrusion Detection and Bandwidth Confusion
- E-Commerce and Security
- Exam

Debates

- Debate Teams Formed By Next Class
  - ★ See Homepage for detalis
- Sample Debate Topics
  - ★ BIRT The notion of the reference monitor does not apply to network security.
  - ★ BIRT A single, global root CA is required for an effective PKI.
  - ★ BIRT IPSec is the best mechanism to provide Internet security for personal electronic commerce.
  - ★ BIRT Steganography can be defeated.
  - ★ BIRT Internet privacy through technical mechanisms can be achieved.
  - ★ BIRT Intrusion detection is the best way to protect against insider malfeasance.
  - ★ BIRT The problem of authentication through firewalls is easily solved.
  - ★ BIRT Key Escrow cannot work in large, dynamic organization
  - ★ BIRT Corruption of machines by low integrity executables renders enforcement of confidentiality policies technically infeasible

Grading of Debates

- 15% of Course Grade
- Clarity of Argument and Preparation for Debate Count more than winning or losing
- Three Debate Evaluations
  - ★ Mine
  - ★ Instant feedback from class in last 5 min of hour
  - ★ Debate evaluations provided within a week of debate
    - also includes a potential quiz or exam question based on debate
- On-line evaluations for the class of the future?
  - ★ Considerations: ease of use, security, mobility

Projects

- 20% of Course Grade
- See web page for details
- Objectives for Projects:
  - ★ Allow you to look at a particular topic in depth
  - ★ Get your hands dirty in the lab (optional)
    - Systems are available and we will attempt to provide you with adequate resources within reason
  - ★ Figure out how to describe something in simple terms
- Caveat: no projects on how to break things -- projects should focus on improving security

Information Assurance

- Ethics and Morals
- Legal Issues
- Physical Security
- Procedural Security
- Personnel Security
- Emanations Security
- Communications Security
- Platform Security

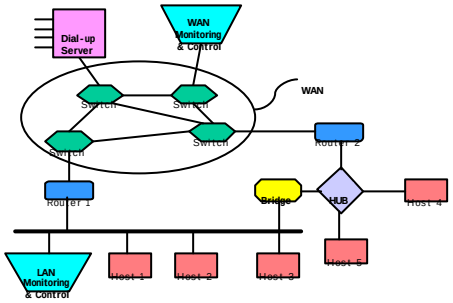
Why Network Security?

- Distributed Systems Rely on Secure Communications and Platforms
- Network Security Complements Physical Security
  - Physical measures cannot be applied to highly distributed networks
- Network Security Complements Platform Security
  - Allows trust in platforms to be extended across the network
  - Provides some defense when platforms are insecure

The Internet

- World Wide
  - used by friends and foe
- Basis for most networking
- Administered by many
  - broad range of skills and interest in security
- No uniform security policy
- Huge and Growing (August 1999 statistics)
  - 800 million web pages
  - 141 million documemts indexed
  - 105.4 million total U.S. users
  - 72 million hosts (Feb 2000)

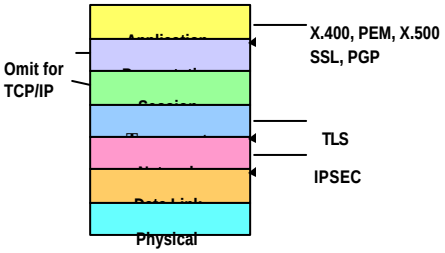
WAN-LAN Attack Targets



Network Components

- Servers
- Communications Medium
- Clients
- Today we have the Internet
- Tomorrow we will have the Super-Embedded Network
  - Hundreds of Devices will be networked together

OSI Layers and Protection Protocols



DoD Network Evolution Affects Security

- Past
  - Dedicated circuits
  - Stovepipe systems
  - Government-developed and produced solutions
  - Risk Avoidance
  - Limited cooperation with industry
  - Government-owned and controlled Security Mgt Infrastructure (SMI)
- Present
  - Significant interconnection
  - Interdependent
  - Commercial technology forms basis of solutions
  - Risk Management
  - Full and open cooperation with industry
  - Global, interoperable Public Key-based SMI

Risk accepted by one is shared by all